PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-023138
(43)Date of publication of application : 22.01.2004

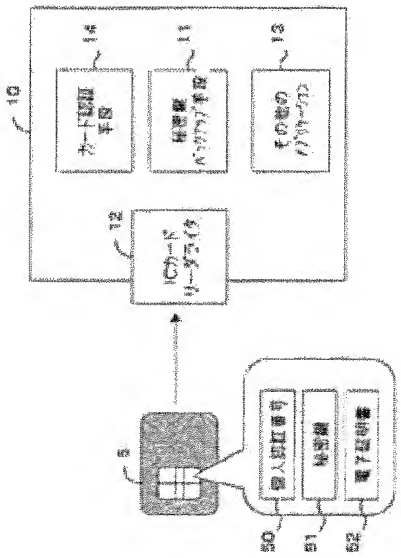
(51)Int.Cl. H04L 9/08
G06F 12/14
G06F 12/16
G06K 17/00

(21)Application number : 2002-171312
(22)Date of filing : 12.06.2002

(71)Applicant : DAINIPPON PRINTING CO LTD
(72)Inventor : ISHIDAIRA IKU

(54) METHOD FOR BACKING UP SECRET KEY AND INFORMATION PROCESSING TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for securely restoring a secret key without a cost increase when an IC card is destroyed or missing.
SOLUTION: This invention in order to solve the problem provides: the method for backing up the secret key recorded on the IC card characterized in that dividing and encrypting data of the original secret key creates a plurality of divided encryption data and a plurality of other IC cards distributingly record the divided encryption data; and an information processing terminal that installs the method on a personal computer.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-23138
(P2004-23138A)
(43)公開日　平成16年1月22日(2004.1.22)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/08	H04L	9/00	601Z	5B017
G06F	12/14	G06F	12/14	310H	5B018
G06F	12/16	G06F	12/14	320B	5B058
G06K	17/00	G06F	12/16	310M	5J104
		G06K	17/00	B	

審査請求 未請求　請求項の数 6　OL　（全 7 頁）

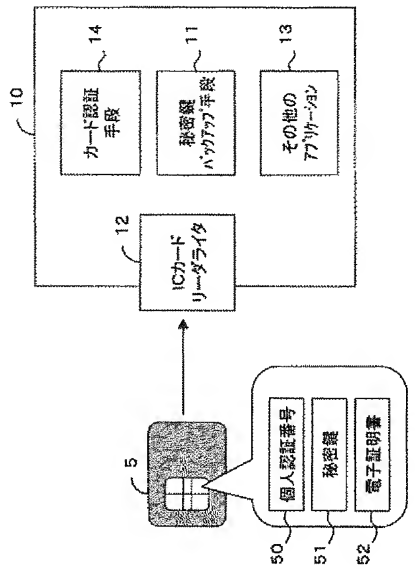
(21)出願番号　特願2002-171312(P2002-171312)
(22)出願日　平成14年6月12日(2002.6.12)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100111659
弁理士　金山　聡
(72)発明者　石平　郁
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

Fターム(参考)　5B017 AA03 BA07 BA10 CA05 CA14
5B018 GA04 HA04 MA24
5B058 CA01 KA02 KA04 KA08 KA35
YA20
5J104 AA16 EA04 EA20 NA02 NA35

(54)【発明の名称】秘密鍵のバックアップ方法および情報処理端末

(57)【要約】
【課題】ＩＣカードを破損、紛失した場合に、安全にコストをかけずに秘密鍵を復旧する仕組みを提供することを課題とする。
【解決手段】ＩＣカードに記録されている秘密鍵のバックアップをとる方法であって、元の秘密鍵のデータを分割して暗号化した複数の分割暗号化データを作成し、他の複数のＩＣカードに前記分割暗号化データを分散して記録させることを特徴とする秘密鍵のバックアップ方法および、この方法をパソコン上に実装した情報処理端末により上記課題を解決する。
【選択図】　図１



【特許請求の範囲】
【請求項1】
ＩＣカードに記録されている秘密鍵のバックアップをとる方法であって、秘密鍵のデータを分割して暗号化した複数の分割暗号化データを作成し、他の複数のＩＣカードに前記分割暗号化データを分散して記録させることを特徴とする秘密鍵のバックアップ方法。
【請求項2】
請求項１に記載の秘密鍵のバックアップ処理方法において、前記分割暗号化データを他の複数のＩＣカードに分散して記録する際、他の複数のＩＣカードの幾つかが失われても元の秘密鍵を復元できるようにするために、前記分散暗号化データを冗長性を持たせて分散して記録することを特徴とする秘密鍵のバックアップ方法。
【請求項3】
請求項１または請求項２に記載のバックアップ処理方法における秘密鍵のバックアップ処理、および、バックアップをとった秘密鍵の復旧処理を実行する秘密鍵バックアップ手段を備えた情報処理端末。
【請求項4】
請求項３に記載の情報処理端末において、ＩＣカードに記録されている個人認証情報により、そのＩＣカードの所有者が当該情報処理端末を使用できるかどうかを決めるユーザー認証手段を備えており、前記秘密鍵バックアップ手段は、秘密鍵のバックアップを行う際、当該情報処理端末の使用を許可されているユーザーのＩＣカードにのみ、前記分割暗号化データを分散して記録させることを特徴とする情報処理端末。
【請求項5】
請求項４に記載の情報処理端末において、前記秘密鍵バックアップ手段は、ＩＣカードから読み出した秘密鍵を所定の分割数で分割しさらに適当な方式により暗号化して前記分割暗号化データを作成する機能、および前記分割暗号化データから元の秘密鍵を復元する機能を備えたものである情報処理端末。
【請求項6】
請求項１または請求項２に記載のバックアップ処理方法において使用されるＩＣカードであって、分割数を含むバックアップコマンドを受けつけた場合に、秘密鍵を所定の分割数で分割しさらに適当な方式により暗号化して前記分割暗号化データを作成して、パソコン側に返答する機能、および復元コマンドとともに一揃いの分割暗号化データを与えられた場合に、元の秘密鍵を復元する機能を備えたＩＣカード。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ＩＣカードにより限定した人のみ利用できるパソコン環境内で、ＩＣカードに記録された秘密鍵のバックアップ、および、逸失したＩＣカードに記録されていた秘密鍵の復元に関する。
【０００２】
【従来技術】
ＰＫＩ（Ｐｕｂｒｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ：公開鍵暗号方式によるデジタル署名を用いた電子文書の認証の仕組み）で利用される秘密鍵はＩＣカードに保管される場合がある。秘密鍵は電子環境における、個人の実印を意味する重要なものであり、絶対に漏洩してはならないので、ＩＣカードに保管する場合は、通常、鍵のバックアップはとらない。一方、秘密鍵のバックアップを取る場合は、そのデータが漏洩されないよう機器の設置、運用に関して特別な配慮が必要である。
【０００３】
秘密鍵や電子証明書を記録したＩＣカードが破損、紛失した場合は、秘密鍵のバックアップがなければ、これに格納された秘密鍵、電子証明書で署名、暗号化した情報が利用できなくなる。又、秘密鍵のバックアップを取っているとしても、安全に保管するための機器の設置、運用などが必要で多大な労力をかけている。これを怠るとセキュリティが著しく

低下する。
【０００４】
【発明が解決しようとする課題】
ＰＫＩの普及が進むことにより、個人の秘密鍵、電子証明書をＩＣカードに保管して利用する人がますます増えてくるものと予想される。それに伴い、秘密鍵、電子証明書を記録したＩＣカードを破損、紛失した場合に、安全にコストをかけずに秘密鍵を復旧する仕組みを用意しておく必要がある。
【０００５】
本発明はこのような問題点を考慮してなされたものであり、ＩＣカードを破損、紛失した場合に、安全にコストをかけずに秘密鍵を復旧する仕組みを提供することを課題とする。
【０００６】
【課題を解決するための手段】
課題を解決するための第１の発明は、
ＩＣカードに記録されている秘密鍵のバックアップをとる方法であって、元の秘密鍵のデータを所定の分割数により分割して暗号化した複数の分割暗号化データを作成し、他の複数のＩＣカードに前記分割暗号化データを分散して記録させることを特徴とする。
【０００７】
第１の発明の方法における望ましい態様は、前記分割暗号化データを他の複数のＩＣカードに分散して記録する際、他の複数のＩＣカードの幾つかが失われても元の秘密鍵を復元できるようにするために、前記分散暗号化データを冗長性を持たせて分散して記録することを特徴とする秘密鍵のバックアップ方法である。
【０００８】
課題を解決する第２の発明は、第１の発明の方法に係る秘密鍵のバックアップ処理、および、バックアップをとった秘密鍵の復旧処理を実行する秘密鍵バックアップ手段を備えた情報処理端末である。
【０００９】
第２の発明の第２の態様は、第２の発明に係る情報処理端末において、ＩＣカードに記録されている個人認証情報により、そのＩＣカードの所有者が当該情報処理端末を使用できるかどうかを決めるユーザー認証手段を備えており、前記秘密鍵バックアップ手段は、秘密鍵のバックアップを行う際、当該情報処理端末の使用を許可されているユーザーのＩＣカードにのみ、前記分割暗号化データを分散して記録させることを特徴とする情報処理端末である。
【００１０】
第２の発明の第３の態様は、第２の発明の第２の態様に係る情報処理端末において、前記秘密鍵バックアップ手段は、ＩＣカードから読み出した秘密鍵を所定の分割数で分割しさらに適当な方式により暗号化して前記分割暗号化データを作成する機能、および前記分割暗号化データから元の秘密鍵を復元する機能を備えることを特徴とした情報処理端末である。
【００１１】
課題を解決する第３の発明は、第１の発明に係るバックアップ処理方法において使用されるＩＣカードであって、情報処理端末から分割数を含むバックアップコマンドを受けつけた場合に、内部に保持している秘密鍵を所定の分割数で分割しさらに適当な方式により暗号化して分割暗号化データを作成して情報処理端末側に返答する機能、および、情報処理端末から復元コマンドとともに一揃いの分割暗号化データを与えられた場合には、元の秘密鍵を復元して内部に保持する機能を備えたことを特徴とするものである。
【００１２】
【発明の実施の形態】
以下図面を用いて、本発明の一実施形態である暗号システムを説明してゆく。ここで暗号システムとはＰＫＩを実現する一組の情報処理端末とＩＣカードを指す。図１は本発明に係る暗号システムの一実施形態である暗号システム１の全体構成を説明するブロック図で

ある。暗号システム１は、秘密鍵バックアップ手段１１、カード認証手段１４およびその他のアプリケーションプログラム１３、ＩＣカードリーダライター１２を備えたコンピュータ１０と個人認証番号５０および秘密鍵５１、電子証明書５２を予め記録してあるＩＣカード５とから構成される。尚、コンピュータ１０には図示してはいないが、利用者に対話インターフェースを提供するモニタディスプレイおよびマウス若しくはキーボード等の入力装置が接続されている。以下図面を用いて暗号システム１を説明してゆく。

【００１３】

パソコン１０はＩＣカードに記録されている個人認証番号より利用者を限定し、利用できないＩＣカード５がリーダライタに挿入された場合は、パソコンを利用させない仕組みを持つものとする。ＩＣカード５がＩＣカードリーダライタ１２に挿入されない場合も、利用させない。ＩＣカード５がＩＣカードリーダライタ１２に挿入されると、カード認証手段１４が自動的に起動され、そのカードの個人認証番号を検査して、上記判定を行う。

【００１４】

ＩＣカード５には所有者の個人認証番号５０、秘密鍵５１および電子証明書５２が記録されている。尚、以下の記載および図面において、カードの持ち主ＡまたはＢ等を特定してＩＣカード５ａ、５ｂなどとも記す。ＩＣカード５というときは持ち主を限定しないでＩＣカードに言及する場合である。他の符号においても同様である。

【００１５】

秘密鍵バックアップ手段１１は、ＩＣカードリーダライタ１２に挿入されているＩＣカード５に記録されている秘密鍵５１のバックアップおよび復元処理を行うアプリケーションプログラムである。

【００１６】

以下秘密鍵のバックアップを行う場合の手順を説明する。

▲１▼ＩＣカードの個人認証番号によりパソコン１０の利用を許可された利用者Ａが秘密鍵　バックアップ手段１１を起動し、秘密鍵５１のバックアップを指示する。秘密鍵バックアップ手段１１は、秘密鍵５１をいくつに分割するかをそのパソコンを利用可能な登録ユーザー数以下で任意に決定する。この分割数は利用者Ａが任意に決めてもよい　。

▲２▼秘密鍵バックアップ手段１１は、ＩＣカード５に対して、秘密鍵５１のバックアップ　コマンドを指令することで、ＩＣカード５から分割、暗号化された秘密鍵を取り出し安全な方法でパソコン内に保管する。例えば分割数を３とした場合は、バックアップコマンドに分割数３をパラメータとして与えてＩＣカードに指令する。ＩＣカード５　は、秘密鍵５１を３分割し暗号化した秘密鍵分割データ６１、６２、６３を秘密鍵バ　ックアップ手段１１に応答する。

▲３▼また、ＩＣカード５の持ち主が新しいＩＣカードに秘密鍵データを復元する時に、持　ち主が同一であることを検証するために必要な情報を秘密鍵分割データ６１、６２、６３とともに記録する。例えばＩＣカード５に記録されている個人認証番号を記録する。図２はこの状態を示す。図２において、パソコン１０内には、利用者Ａの秘密鍵　のバックアップのために管理されるデータの集合１１０が作成され、この中に秘密鍵　分割データ６１、６２、６３および利用者Ａの個人認証番号５０ａが記録保持される　。

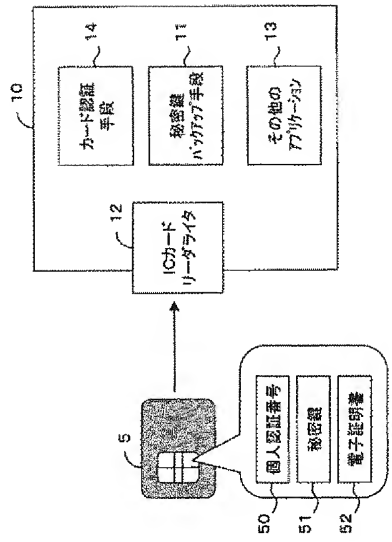
▲４▼次に利用者Ａ以外の人（利用者Ｂ）が、この環境を利用するときに、利用者Ａの秘密　鍵の分割データの１つである６１を自動的に利用者ＢのＩＣカード５ｂに書きこみ、　ＩＣカード５ｂに書かれた個人認証番号５０ｂを取出し安全な方法（暗号化など）で記憶しておく。この時、利用者ＢのＩＣカードに書きこんだ秘密鍵の分割データ６１　はデータ集合１１０から消去される。図３はこの状態を示した図である。

▲５▼パソコン１０を使用できる他の利用者（利用者Ｃ，Ｄ）がこの環境を利用するときに　、秘密鍵の分割データがなくなるまで上記▲４▼の動作を繰り返す。分割データ６０、６　１、・・が全て、他のＩＣカードへ書きこまれると、利用者Ａの秘密鍵のバックアッ　プは終了となる。パソコン１０のデータ集合１１０には、消去された分割データ６０　、６１、・・の代わりに、それらが書込まれた先のＩＣカードを特定する個人認証番号５０ｂ、５０ｃ、５０ｄが残る。図４は、この状態のパソコン１０およびデータ集　合

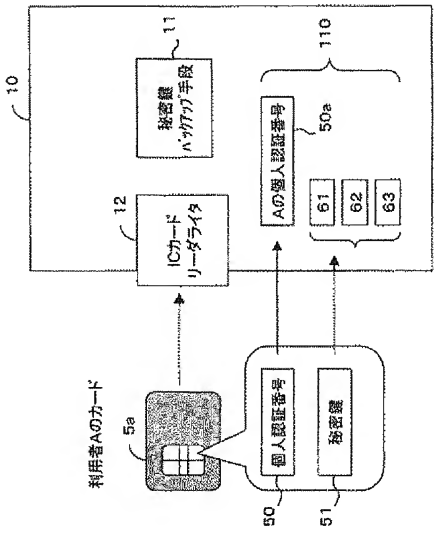
１１０の様子を示している。
【００１７】
ＩＣカード紛失時の秘密鍵の復元手順は次の通りである。
▲６▼ＩＣカードを破損、紛失した利用者Ａは、新しいＩＣカードを準備し、紛失したＩＣ　カードの秘密鍵のバックアップをとったパソコン１０にて、秘密鍵の復元を指示する。
▲７▼秘密鍵バックアップ手段１１が起動する。新しいＩＣカードの持ち主が以前、秘密鍵　のバックアップを取った本人であることの認証を行う。これは▲３▼で残したデータ集合　１１０内に記録されている個人認証番号５０ａが新しいＩＣカードに記録されている　個人認証番号５０と一致するかどうかで判断する。
▲８▼復元を指示された、秘密鍵バックアップ手段１１は、以降、上記▲４▼で記憶したＩＣカ　ードに書かれた固有情報の所有者がこの環境を利用する毎に（これはデータ集合１１　０内に記録されている個人認証番号５０ｂ、５０ｃ、・・に一致する個人認証番号を　カード内に含んでいるかによりチェックできる）、以前ＩＣカードに書かれた所有者　Ａの分割された秘密鍵データ６０、６１、・・を取り出し、安全な方法（暗号化されたままの状態）で読み出しデータ集合１１０に保持する。
▲９▼上記▲３▼で決定した全ての分割秘密鍵データ６０、６１、６３が準備できた段階で、所　有者Ａの新しいＩＣカードをリーダライタに挿入し、秘密鍵バックアップ手段１１を　起動させ、組み立て合成を指示するコマンドとともに分割秘密鍵データ６０、６１、　６３をＩＣカード５に送り付ける。すると新しいＩＣカードの中で秘密鍵が再構成される。
【００１８】
利用者Ａの秘密鍵を復元するためには、秘密鍵バックアップ手段１１が書きこんだ他のＩＣカードが全て必要になるので、他のＩＣカードがなくなっている場合を考慮して、▲４▼の書きこみ処理を、２重化、３重化してなど、適当な冗長性を持たせるようにしてもよい。
【００１９】
上記▲２▼において、ＩＣカード５は、秘密鍵のバックアップコマンドを受けると、分割、暗号化されたデータ６１、６２、・・を出力するとしている。これは秘密鍵を分割しかつ暗号化する手段およびその逆処理を行い再構成する手段をＩＣカード５の内部に備えていることを想定している。実施態様としてはこのような態様に限られるわけではない。ＩＣカード５から出力されるのは秘密鍵データそのもので、分割暗号化はパソコン側で、即ち秘密鍵バックアップ手段１１が行ってもよい。あるいは、分割と暗号化をＩＣカード５と秘密鍵バックアップ手段１１で分担して行ってもよい。いずれの態様でも、秘密鍵の分割データが暗号化されたもの、または、秘密鍵を暗号化したデータを分割したものが得られればよい。
【００２０】
【発明の効果】
以上詳しく説明したように、本発明に係る暗号システムを用いれば、秘密鍵、電子証明書を記録したＩＣカードを破損、紛失した場合に、安全にコストをかけずに秘密鍵を復旧するという顕著な効果を奏する。
【図面の簡単な説明】
【図１】本発明に係る暗号システム１の全体構成ブロック図である。
【図２】暗号システム１における秘密鍵のバックアップ動作を説明する図である。
【図３】暗号システム１における秘密鍵のバックアップ動作を説明する図である。
【図４】暗号システム１における秘密鍵の復旧動作の初期段階を説明する図である。
【符号の説明】
５　　ＩＣカード
１０　　パソコン
１１　　秘密鍵バックアップ手段

１２　　ＩＣカードリーダライタ
１３　　その他のアプリケーション手段
１４　　カード認証手段
５０　　個人認証番号
５１　　秘密鍵
６１　　分割暗号化データ
６２　　分割暗号化データ
６３　　分割暗号化データ
１１０　バックアップ管理データの集合

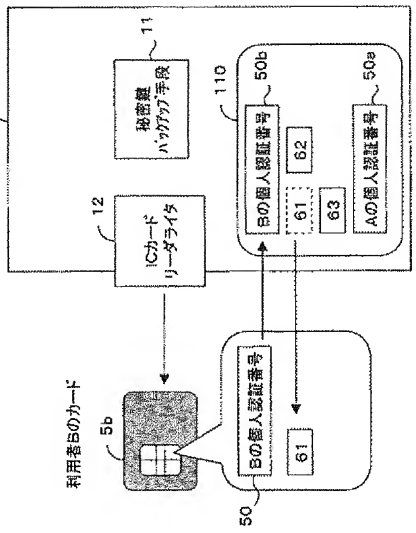
【図1】



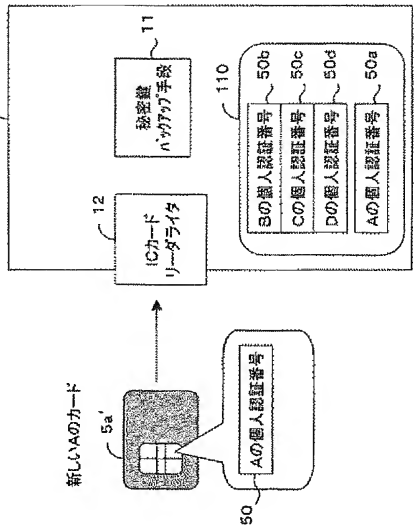
【図2】



【図3】


10
11
秘密鍵
バックアップ手段
12
ICカード
リーダライタ
110
50b
Bの個人認証番号
61
62
63
50a
Aの個人認証番号
利用者Bのカード
5b
Bの個人認証番号
61
50

【図4】


10
11
秘密鍵
バックアップ手段
12
ICカード
リーダライタ
110
50b
Bの個人認証番号
50c
Cの個人認証番号
50d
Dの個人認証番号
50a
Aの個人認証番号
新しいAのカード
5a'
Aの個人認証番号
50